

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-072720

(43)Date of publication of application : 17.03.2005

(51)Int.Cl.

H04L 12/56

H04L 12/28

(21)Application number : 2003-296657 (71)Applicant : SONY CORP

(22)Date of filing : 20.08.2003 (72)Inventor : YANO YUICHI

(54) COMMUNICATION NETWORK SYSTEM COMMUNICATION PATH SELECTING APPARATUS AND INFORMATION COMMUNICATION MEANS

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication system capable of utilizing the optimum channel corresponding to the quality necessary for an application in a communication network having a plurality of channels for performing communication from a terminal device connected to a mesh-like network configured by mutually connecting a plurality of nodes to an external network.

SOLUTION: When the terminal device connected to the mesh-like network configured by mutually connecting a plurality of nodes accesses the external network via this mesh-like network. In this case if there are many channels from the mesh-like network to the external network a node directly connected to the terminal device collates the communication quality required for transferring the data inputted from this terminal device with the communication quality of each of the communication channels and selects the optimum communication channel for transferring the data.

CLAIMS

[Claim(s)]

[Claim 1]

Two or more nodes are the communication network systems which access an external network via said mesh network from a terminal unit linked to a mesh network constituted by connecting mutually

When two or more communication paths from said mesh network to an external network exist A node which carries out direct continuation to said terminal unit

compares communication quality required of transmitting data inputted from said terminal unit and communication quality of each communication path and has a communication-path selecting means which chooses the optimal communication path for transmitting the data concerned.

A communication network system characterized by things.

[Claim 2]

In the communication network system according to claim 1

A tunnel setting-out means to set a tunnel as a communication path between a node which carries out direct continuation of said communication-path selecting means to said terminal unit and a server of said external network

An application classification quality record means to record communication quality which application software classification requires beforehand

A quality identification means to supervise communication quality of each communication path

A communication-path quality record means to record quality information acquired by the surveillance of said quality identification part

It is judged whether each data inputted into said node from 1 or two or more terminal units corresponds to which application software classification currently recorded on said application classification quality record means. Quality information currently recorded on said application classification quality record means and said communication-path quality record means is compared and it has with a course discriminating means which specifies 1 or two or more communication paths which secure quality which said each data requires

Said each data is outputted to said specified communication path.

A communication network system characterized by things.

[Claim 3]

In the communication network system according to claim 2

Said tunnel setting-out means is classified and set to either a tunnel which uses said tunnel only for data communications of a specific application software classification or a tunnel which can be used for data communications of arbitrary application software classification.

A communication network system characterized by things.

[Claim 4]

It is a node which carries out direct continuation to said terminal unit when two or more nodes access an external network via said mesh network from a terminal unit linked to a mesh network constituted by connecting mutually. When two or more communication paths from said mesh network to an external network exist, communication quality required of transmitting data inputted from said terminal unit and communication quality of each communication path are compared and the optimal communication path for transmitting the data concerned is chosen.

A communication-path selecting arrangement characterized by things.

[Claim 5]

In the communication-path selecting arrangement according to claim 4

A tunnel setting-out means to set a tunnel as a communication path between a node which carries out direct continuation of said communication-path selecting means to said terminal unit and a server of said external network

An application classification quality record means to record communication quality which application software classification requires beforehand

A quality identification means to supervise communication quality of each communication path

A communication-path quality record means to record quality information acquired by the surveillance of said quality identification means

It is judged whether each data inputted into said node from 1 or two or more terminal units corresponds to which application software classification currently recorded on said application classification quality record means. Quality information currently recorded on said application classification quality record part means and said communication-path quality record means is compared and it has a course discriminating means which specifies 1 or two or more communication paths which secure quality which said each data requires

Said each data is outputted to said specified communication path.

A communication-path selecting arrangement characterized by things.

[Claim 6]

In the communication-path selecting arrangement according to claim 5

Said tunnel setting-out means is classified and set to either a tunnel which uses said tunnel only for data communications of a specific application software classification or a tunnel which can be used for data communications of arbitrary application software classification.

A communication-path selecting arrangement characterized by things.

[Claim 7]

Two or more nodes are the information-and-telecommunications methods which access an external network via said mesh network from a terminal unit linked to a mesh network constituted by connecting mutually

A step which sets a tunnel as a communication path between a node which carries out direct continuation to said terminal unit as said communication path and a server of said external network when two or more communication paths from said mesh network to an external network exist

A step which records communication quality which application software classification requires beforehand

A step which supervises communication quality of a tunnel set as said communication path

A step which records quality information of said tunnel obtained by surveillance

It is judged whether each data inputted into said node from said terminal unit

corresponds to which application software classification currently recorded on said application classification quality record means A step which specifies 1 or two or more communication paths which secure communication quality which compares communication quality which said application classification requires and communication quality of said tunnel and said data requires

It has a step which outputs said data to said specified communication path.

An information-and-telecommunications method characterized by things.

[Claim 8]

In an information-and-telecommunications method according to claim 7

In a step which sets up said tunnel it classifies and sets to either a tunnel which uses said tunnel only for data communications of a specific application software classification or a tunnel which can be used for data communications of arbitrary application software classification.

An information-and-telecommunications method characterized by things.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[Field of the Invention]

[0001]

This invention relates to the communication network system communication-path selecting arrangement and the information-and-telecommunications method of accessing the server on an external network from the terminal unit which joins the network which comprises a node connected to mesh shape for example and performing information and telecommunications.

[Background of the Invention]

[0002]

Although one of the radio art in recent years has an ad hoc network This ad hoc network has taken the gestalt (multi-hop communication) which connects many terminals without the intervention of an access point mutually forms a network in mesh shape using radio art and enables use of two or more courses. For this reason a base station and an access point become unnecessary can build a network cheaply at a place without such an infrastructure and are effective in an ad hoc network as a certain limited means of construction of a network simple within the area.

[0003]

However an ad hoc network is difficult to leave behind technical problem and to secure the steady quality of a communication path — unlike a wired network a communication rate changes every moment — in order that each node may carry out wireless connection autonomously and may constitute a network.

[0004]

As one of measures according to the communication rate of the data within a network To the thing controls starting of application software (application is called hereafter.) and it was made to operate application by an always good operating state. For example the data-communications rate between the client terminal within a network and a host terminal is measured When the communication rate is judged to be less than the communication rate which operates the predetermined application of a client terminal normally based on the measurement history there is art which restricted starting of the predetermined application of a client terminal (for example refer to patent documents 1.).

[Patent documents 1] JP2003-122672A

[Description of the Invention]

[Problem(s) to be Solved by the Invention]

[0005]

Corresponding [however] to the communication rate produced by the thing of a description measuring the communication rate of the communication line between the terminals made into the object in a network to the patent documents 1 It controls so that only the application which can start in a client terminal and can be operated normally can start and when the communication rate which application requires was not obtained there was inconvenience that the target application could not be started.

[0006]

In an ad hoc network only the optimal path for each node is calculated and it communicates using the course. However in the actual condition of using general TCP/IP (Transmission Control Protocol/Internet Protocol) even if two or more nodes accessed out of an ad hoc network in that case exist. The thing with one available session by application software etc. became only one course and since it was not able to distribute at the time of the same session there was inconvenience that the advantage which two or more courses have could not be employed efficiently.

[0007]

In a communication network with two or more courses which perform communication with an external network from the terminal unit linked to the mesh network constituted by two or more nodes connecting this invention mutually in view of this point It aims at proposing the communication method which can use the optimal course corresponding to the quality which application needs.

[Means for Solving the Problem]

[0008]

In order to solve an aforementioned problem and to attain the purpose this invention When two or more nodes access an external network via this mesh network from a terminal unit linked to a mesh network constituted by connecting mutually When two or more communication paths from a mesh network to an external network exist Communication quality required of a node which carries out direct continuation to a terminal unit transmitting data inputted from this terminal unit and

communication quality of each communication path are compared. Choose the optimal communication path for transmitting the data concerned and more specifically a tunnel setting-out means to set a tunnel as a communication path between a node which carries out direct continuation to a terminal unit and a server of an external network. An application classification quality record means to record communication quality which application software classification requires beforehand. A quality identification means to supervise communication quality of each communication path and a communication-path quality record means to record quality information acquired by the surveillance of this quality identification means. It is judged whether each data inputted into this node from 1 or two or more terminal units corresponds to which application software classification currently recorded on said application classification quality record means. Quality information currently recorded on this application classification quality record means and this communication-path quality record means is compared. It has with a course discriminating means which specifies 1 or two or more communication paths which secure quality which each data requires and each data is outputted to this specified communication path.

[0009]

When two or more communication paths from a mesh network to an external network exist according to this invention. By comparing communication quality acquired by supervising communication quality and each communication path which are required of a node which carries out direct continuation to a terminal unit transmitting data inputted from the terminal unit. A communication path with quality needed for transmitting the target data is chosen and optimal course is used.

[0010]

This invention classifies and sets the above-mentioned tunnel setting-out means to either a tunnel which uses a tunnel only for data communications of a specific application software classification or a tunnel which can be used for data communications of arbitrary application software classification.

[0011]

In classifying a tunnel into either for general which can be used for application software the object for immobilization or arbitrary used for a certain specific application software in this invention when setting up a tunnel. Only by specifying application software classification of inputted data a tunnel (communication path) can be appropriately assigned according to quality which application software classification requires.

[Effect of the Invention]

[0012]

By acquiring the information about communication quality set up in order to perform communication to an external network from the network of mesh shape [ad hoc for example] such as the zone and time delay of each course (tunnel) and a packet loss rate according to this invention. Streaming data of download voice data a video

data text data etc. which are inputted from a terminal unit can choose the suitable course for each communication and effective use of the zone of each course is attained. Therefore the steady communication quality at the time of accessing to an external network is securable from a mesh network.

[0013]

By what a tunnel is classified and set for to general [which can be used for application software the specific object for application software or arbitrary]. Only by specifying the application software classification of the inputted data a tunnel (communication path) can be appropriately assigned according to the quality which application software classification requires and the zone of each course can be used effectively more efficiently.

[Best Mode of Carrying Out the Invention]

[0014]

Hereafter the example of the 1 embodiment of this invention is explained with reference to drawing 1 – drawing 12.

This example from the terminal unit which has joined the independence distributed network which realizes communication by combining between nodes provided with a gate way function with ad hoc. Have considered it as the example applied when external network such as the Internet were accessed and the ad hoc example [this] communication network itself. The so-called network of approximately mesh shape (mesh) is constituted using the existing art such as MANET (Mobile Ad-hoc Networks).

[0015]

The general drawing of the communication network system of this example is shown in drawing 1.

1 is a terminal unit connectable with the ad hoc network which comprises the nodes 2–7 provided with the gate way function. The nodes 2–7 carry out interconnection to two or more nodes which exist in the circumference and the network (NW is called hereafter.) 10 is formed by IP (Internet Protocol) in this example. 8 is a server which is provided on the external networks (the exterior NW is called hereafter.) 20 such as the Internet and receives the node 6 or the needed information from 7 and data on an ad hoc network. This server 8 functions also as a tunnel server which forms the node in NW 10 and the tunnel mentioned later. 9 is a terminal unit connected with the server 8 so that communication is possible. In this example as for an access node and other the nodes 6 and 7 linked to an access line are general nodes.

[0016]

The software module composition of the node which forms the mesh network of this example is shown in drawing 2.

So that it may be shown among a figure The MANET module 30 the tunnel setting-out module 31 the node authentication module 32 the quality identification module 33 an application database. (The application DB is called hereafter.) 34 a tunnel information database. (The tunnel DB is called hereafter.) It shall be constituted by 35 the routing

table 36 the packet input module 37 the packet judging module 38 and the packet output module 39 and shall be stored in ROM (Read Only Memory) which is not illustrated.

[0017]

The tunnel setting-out module 31 and the node authentication module 32 function as a tunnel setting-out means and transmit and receive burrow information a tunnel setting request node attestation etc. which are needed when performing tunnel setting out. And the quality identification module 33 which functions as a quality identification means The quality identification module 33 in a general node like the node 2 which receives tunnel setup information from the tunnel setting-out module 31 for example carries out direct continuation to a terminal unit While supervising periodically the communication quality of the tunnel which actually set up connection and registering the quality information into tunnel DB35 comparison with the communication quality which the application classification registered into application DB34 mentioned later requires etc. are performed.

[0018]

Application DB34 Application software. (Application is called hereafter.) It functions as an application classification quality record means to record the communication quality which classification requires As it is a database which arranges and stores the quality which the data which passes along a node requires for every application for example is shown in below-mentioned drawing 11 Information including application classification DSCP (DiffServ Code Point) a time delay a packet loss rate a transmission band the number of session etc. is registered. When a case so that this number of sessions may communicate by connecting two or more terminal units to the node 2 of drawing 1 for example is assumed in the same application classification the node 2 expresses the controllable number of sessions simultaneously.

[0019]

So that tunnel DB35 may function as a communication-path quality record means and it may be shown in the quality information acquired by supervising regularly the tunnel set up with the quality identification module 33 for example below-mentioned drawing 12 Information including the measuring times of ID of the access node on a course an IP address a time delay a packet loss rate a quota zone and communication quality etc. is stored.

[0020]

The routing table 36 holds the path table in an ad hoc network and the set-up path table of a tunnel in this example as general routing.

[0021]

While the MANET module 30 builds a network independently with an adjoining node For example communication by a MANET routing protocol which is variously proposed by the workgroup (WG) of IETF (Internet Engineering Task Force) based on the path table of the above-mentioned routing table 36 is performed.

[0022]

The packet input module 37 processes the packet inputted from LAN (Local Area Network) WAN (Wide Area Network) etc. in the general node side. An access node is also the same. The packet input module 37 supplies the packet which received from the outside to the packet judging module 38.

[0023]

The packet judging module 38 functions as a course discriminating means. It specifies through which tunnel (communication path) the information on the packet which compared application DB 34 and tunnel DB 35 and was extracted with the packet input module 37 is transmitted to an external network and transmits to the packet output module 39. The packet output module 39 outputs a packet to the course specified by the packet judging module 38.

[0024]

These modules of each node constitute a control section with the node authentication module 32, the tunnel setting-out module 31, the quality identification module 33, and the MANET module 30. The packet input module 37, the packet judging module 38, and the packet output module 39 constitute a packet treating part. A control section and a packet treating part perform suitable communications control of a packet according to the information stored in the application database 34, the tunnel information database 35, and the routing table 36.

[0025]

The main functions in the general node of each node constituted are as follows like ****.

1. Build an ad hoc network independently using the existing art.
2. Receive broadcasting from an access node and set up a tunnel based on the information.
3. Perform the connection request by tunneling to an access node.
4. Supervise the quality of the connected tunnel periodically.
5. Hold DB in which the quality which the application outputted and inputted requires is stored.

DB in which the quality of the tunnel currently supervised by 6. is stored is held.

7. Hold the channel information of an ad hoc network and a tunnel.
8. LAN/WAN etc. process the packet inputted from other nodes.
9. Determine the destination of a packet based on the information on the packet extracted with the packet input module.
10. Output a packet to the course specified by the packet judging module.

[0026]

The main functions in an access node are as follows.

1. Build an ad hoc network independently using the existing art.
2. Advertise the information on the access line which self has connected and the communication band permitted to each node in an ad hoc network with

techniques such as broadcasting.

3. The connection request from a general node is attested.
4. Hold the channel information of an ad hoc network and a tunnel.
5. LAN/WAN etc. process the packet inputted from other nodes.
6. Determine the destination of a packet based on the information on the packet extracted with the packet input module.
7. Output a packet to the course specified by the packet judging module.

[0027]

With reference to drawing 3 the signal transduction performed between the access node in a network and a general node is explained.

First an access node broadcasts periodically the default route (default communication path) information used from the tunnel setting-out module 31a as burrow information to an unspecified general node (distribution). A general node receives default route information by the tunnel setting-out module 31a and performs the connection (tunnel setting out) demand by tunneling to an access node based on the information.

[0028]

According to the tunnel setting request from a general node as for an access node the tunnel setting-out module 31b outputs a node authentication request signal to the node authentication module 32b. The node authentication module 32b reports that node attestation is carried out to the general node which required tunnel setting out. The tunnel setting-out module 32a which received the node authentication notification carries out the response to node attestation to an access node if the zone of a tunnel is not clearly narrow or problems like a packet loss rate is large are not seen for example.

[0029]

An access node receives the response of the node attestation from a general node with the node authentication module 32b supplies a tunnel setting-out enabling signal to the tunnel setting-out module 31b and transmits tunnel setup information to a general node from the tunnel setting-out module 31b.

[0030]

And while registering with the routing table 36 which received tunnel setup information by the tunnel setting-out module 31a in the general node and was shown in drawing 2 The quality identification module 33a performs performance monitoring of a tunnel regularly based on this tunnel setup information and registers the quality of that tunnel into tunnel DB 35a as tunnel information. And although mentioned later the quality identification module 33a judges compatibility with the quality which the tunnel information registered with reference to the application information registered into application DB 34a and application classification require QoS (Quality of Service) is realized.

[0031]

Next tunnel setting out of the communication network system of this example is

explained with reference to drawing 4 -- the explanatory view of sixdrawing 7 and the flow chart of 8.

First each node builds the ad hoc network (NW) 10 independently using the existing art. Each node about specific application Layer 3 header in open systems interconnection reference models such as an IP/ICMP (Internet Control Message Protocol) header And the information on layer 4 header including TCP (Transmission Control Protocol) / UDP (User Datagram Protocol) header And information including the delay zone packet loss rate etc. which the application requires is held as a database as shown in drawing 2.
[0032]

The explanatory view of the default route information distribution at the time of performing tunnel setting out is shown in drawing 4. The access nodes 6 and 7 linked to external NW20 broadcast the default route (default communication path) information used considering the purport that it has connected the outside of NW10 as burrow information to an adjoining node (Step S1). (distribution)
[0033]

In this example the node 2 receives the burrow information on the course which passes along the nodes 6 and 3 as shown in drawing 4 and the course which passes along the nodes 7 and 4. NW10 top may be broadcast regularly when the terminal unit 1 connects with NW10 it may be received and an exchange in the usual IP layer or the exchange by the application layer and any may be sufficient as the default communication data used as the basis of this burrow information.
[0034]

Drawing 5 is an explanatory view of ad hoc network inner tunnel setting out of this example. The node 2 requests tunnel setting out to the access nodes 6 and 7 according to the received default communication data (Step S2). The existing art is used about setting out of a tunnel. In order to prevent tapping within NW10 etc. for example rather than IP-in-IP (RFC 1853) or GRE (RFC 1701). Use in the tunnel mode of IPsec (Security Architecture for Internet Protocol) is more preferred.
[0035]

It is judged whether the access nodes 6 and 7 attest the requested node 2 (Step S3). If it judges that it is unsuitable as a connection object and attestation will be refused it will distinguish whether the predetermined number-of-times attestation of specification went wrong (step S4) and the number-of-times attestation of specification will not have gone wrong it will return to processing of Step S2 and a tunnel request will be repeated. When the number-of-times attestation of specification goes wrong tunnel setting processing is ended. The access nodes 6 and 7 transmit the information on a tunnel to the node 2 when it judges that the node 2 is suitable as a connection object and attestation passes (Step S5).
[0036]

The node 2 judges whether the tunnel information received from the access nodes 6 and 7 is effective for the node 2 (Step S6) and when not effective it ends tunnel

setting processing. When it is judged that it is effective the node 2 sets up a tunnel between the node 2 the node 6 and the node 7 based on the received tunnel information respectively (Step S7).

[0037]

Drawing 6 is an explanatory view of mesh network outer tunnel setting out of this example. The tunnels 11 and 12 stretched between the node 2 and the access nodes 6 and 7 which were connected with the terminal unit 1 are used and a tunnel is further set up between the servers 8 on the external network 20. The node 2 requires tunnel connection towards the server 8 besides NW10 from each tunnels 11 and 12 which set up the default communication path. Under the present circumstances attestation by the server 8 is performed. Apparatus ID of an applicable node and the IP address in NW10 are transmitted to discernment of a node and it is used for attestation.

[0038]

In addition to the usual authenticating processing the tunnel server 8 performs the following registration. Part two or more **** of a communication path are registering them and the IP address used to the node 2 identifies the communication from two or more tunnels as the one flow (flow). The tunnel server 8 removes the header of the packet which arrives from two or more tunnels stretched between the nodes 2 and returns it to one flow based on the above-mentioned IP address.

[0039]

On the occasion of the tunnel setting request from the node 2 if the server 8 judges that it is unsuitable as a connection object it will refuse attestation. If satisfactory as a connection object it will reply judging that it is suitable and permitting attestation to the node 2 and a tunnel will be set up between the node 2 and the server 8 using the tunnel 11. Similarly a tunnel with the node 2 and the server 8 is set up using the tunnel 12 set up in NW10. The set-up tunnel information is registered into the tunnel DB. In the example of drawing 6 two accessible tunnels (communication path) exist in the server 8 of external NW20 from the terminal unit 1 of NW10.

[0040]

Next the steady tunnel surveillance phase which performs performance monitoring of the set-up tunnel is explained.

First the node 2 will carry out additional registration of the information on the tunnel set up newly to the tunnel DB if a tunnel is set up (Step S8). The tunnel addition flow at this time is explained with reference to the flow chart of drawing 8.

[0041]

The node 2 judges whether the application which requires special transfer rules such as streaming data for example exists in the application DB. A node compares the application DB with the tunnel DB and checks whether the tunnel which can secure the communication quality which individual application classification requires exists (Step S21). When special transfer rules do not exist a new tunnel is added to a common tunnel (Step S22). A common tunnel is a tunnel which is not limited to

communication of a specific application use and which is used for the other purposes here. The tunnel for special shall refer to the tunnel used only for a specific application use.

[0042]

Next when the application which requires special transfer rules exists in the application DB when it judges whether the optimal tunnel for these special transfer rules exists (Step S23) and does not exist in the tunnel registered into the tunnel DB including the newly set-up tunnel additional registration of the new tunnel is carried out to a common tunnel (Step S24).

[0043]

When the optimal tunnel exists to special transfer rules by processing of Step S23 when it is one it is judged first whether the one tunnel is a new tunnel (Step S25). When it is a new tunnel it is set as the tunnel for special (for individual) which limited the new tunnel to communication of the application of special transfer rules chiefly and registers with the tunnel DB (Step S26). When it is not a new tunnel an applicable tunnel is set as the tunnel for special and a new tunnel is registered into a common tunnel (Step S27).

[0044]

When the optimal tunnel for the tunnel DB exists to special transfer rules by processing of Step S23 when it is [two or more] it is judged first whether a new tunnel is included in the two or more tunnels (Step S28). When a new tunnel is included a tunnel group including the new tunnel is set as the tunnel for special chiefly limited to communication of the application of special transfer rules when it registers (Step S29) and does not include a new tunnel an applicable tunnel group is set as the tunnel for special and a new tunnel is registered into a common tunnel (Step S30).

[0045]

Thus according to the quality which the application of the data inputted into the node requires a suitable tunnel (communication path) can be immediately chosen from a terminal unit by assigning a tunnel beforehand to the object for general and special and registering with a database.

[0046]

And the tunnel stretched between the servers 8 from the quality identification module of the node 2 is received. For example quality information to which the beacon for a life-and-death check and a quality information demand is periodically transmitted at intervals of 1 second etc. (step S9) and which is answered from the tunnel communication quality response module (not shown) of the server 8 such as a time delay and a packet loss rate is collected and it records on the tunnel DB. When it judges whether there is any reaction from a tunnel to transmission of a beacon at this time (Step S10) there is a reaction and the response to a quality information demand has returned. While reflecting the replied tunnel quality information in a database the shelf-life set up based on the measuring times of drawing 12 is updated (Step S11) it

shifts to processing of Step S8 and steady tunnel surveillance is continued.

[0047]

When there is no reaction from a tunnel within a shelf-life the information on the tunnel is deleted and cut from the tunnel DB (Step S12). For example when a prescribed frequency beacon is transmitted there was no response it was judged as the communication-path down and delete the tunnel from the tunnel DB and it is cut or the quality of a tunnel becomes below a fixed standard it may not correspond under life-and-death surveillance or may be made to cut a tunnel. The quality information of these tunnels is held in a database.

[0048]

In a series of tunnel addition flows of Step S8 how to register first all the tunnels set up newly as a tunnel for general can be considered. That is a general node transmits all the applications using the tunnel for general until it registers the tunnel set up first as a tunnel for generic applications and a tunnel peculiar to application is set up. Henceforth when a new tunnel is set up according to the communication quality of the tunnel which changes every moment it is made to add and register the tunnel as a common tunnel at first to be a process of steady tunnel surveillance and to change a use at any time.

[0049]

A node compares the application DB with the tunnel DB and checks periodically whether the tunnel which can secure the communication quality which individual application classification requires exists. When quality cannot be secured in one tunnel the application is transmitted using the tunnel for general until it is securable. The tunnel for individual can be added until the tunnel for general remains and it becomes one. The situation where there is no tunnel which corresponds if it can respond to all the applications and depends on application classification by leaving at least one tunnel for general and it cannot communicate is avoided.

[0050]

Drawing 9 can show an example in case the terminal unit 1 which the communication network system of this example connects to NW10 communicates with the terminal unit 9 of the external network 20 and can mount it in the following packet format forms.

[0051]

Although this example is an application gestalt of IPsec(tunnel mode)+NAT (Network Address Translation) traversal the server 8 achieves the following function at this time.

- Apparatus ID is seen and it has a function which changes into a suitable IP address.
- Carry out a buffer to a suitable temporal cue method (queue) and send out in order of the sequence number of TCP as much as possible.
- In the case of UDP send out as it is.

[0052]

Assigning [for example] an IP address to each apparatus the node 2 which are an IP

address "IP-z" and apparatus ID "E-ID" and a communication-path selecting arrangement makes the terminal unit 1 an IP address "IP-Z" by NAT. The nodes 6 and 7 linked to an access circuitIt is referred to as the IP address "IP-A" by NATIP-Band the IP address "IP-1" according from external NW20 to NAPT (Network Address Port Translation)and "IP-2" from NW10 siderespectively. The server 8 makes the IP address "IP-3" by NAPTand the terminal unit 9 an IP address "IP-4" further again.

[0053]

When two or more tunnels are stretched from the node 2 to the server 8two or more IP addresses are assigned with methodssuch as round-robin (round-robin) oneandas for the node 2self transmits the data sent from the terminal unit 1 to an available tunnel by 1 packet unit. At this timethe packet information of the communication to the node 2 from the terminal unit 1 is "DATA" and "a TCP header (z->4)." And when the node 2 distributes to two communication paths of the tunnels 11 and 12 and it is transmittedthe packet information of the communication to the node 6 and the node 7 from the node 2It becomes "DATA"an "IP header"an "IPsec header"and a "tunnel IP header"and the "tunnel IP header" for transmitting the inside of the "IPsec header" and tunnel showing the IP address information on the node of the both ends of the tunnels 11 and 12 is added.

[0054]

When transmitted to the server 8 in the exterior NW20 from the node 6the communication packet informationThe information transmitted on NW10 using the tunnels 11 and 12 disappearsand the "UDP header" is added by using UDP as a protocol of communication between NW10 and NW20 hererespectively. The server 8 judges that the source of the packet transmitted from the nodes 6 and 7 based on apparatus ID and a TCP header is a thing from the same node 2and reconstructs the information distributed by the packet unit. Since it is communication by UDP in this example at this timereconstruct in consideration of round-Trip Timeand as information on "DATA" and "a TCP header (3->4)"By transmitting what reconstructed the packet in one communication information to the terminal unit 9the terminal unit 9 can receive the data from the terminal unit 1 from the server 8.

[0055]

When two or more tunnels are stretched from the node 2 with the single server 8It recognizes that it is the tunnel which changes from the same node 2 with apparatus ID of the applicable node 2or IP addresses in NW10and the packet from the same node transmitted via two or more tunnels is reconstructed in one communication. For examplein the case of TCPit is a sequence numberand in the case of UDPPreconstruction in a right order is performed using the difference of round-Trip Time (RTT:Round Trip Time)and it transmits it to the exterior.

[0056]

The terminal unit connected to the node 2 by mounting the above structureTwo or

more courses with an adjoining node can be used since it is possible to make two or more zones distribute one session the burden placed on the communication path per one can be eased and the maximum of transmission speed can be improved substantially. Two or more sessions can be communicated simultaneously.

[0057]

Selection of a communication path when data is inputted from a terminal unit in the communication network system of this example is explained with reference to drawing 12. This drawing 12 sets up the tunnels 24 and 25 respectively while the access nodes 6 and 7 on an ad hoc network connect with the server which the network 22 does not illustrate via the external networks 21 and 23 respectively as compared with drawing 1 drawing 6 – drawing 8 Others are the same composition although the point he is trying to communicate with the terminal unit 9 is different.

[0058]

If it sees from the terminal unit 1 or 9 from each terminal unit data seems to carry out the direct communication of the between with the node 2 and the server on the network 22 which is not illustrated via the tunnels 11 and 24 or the tunnels 12 and 25 but. Actually the data communications between the terminal unit 1 and the terminal unit 9 are performed via a thick line part respectively.

[0059]

When data (packet) has been inputted from the terminal unit 1 the node 2 which is carrying out direct continuation to the terminal unit 1 With reference to the layers L5 such as layers such as layers such as IP/ICMP header 3 header and TCP/UDP header 4 header and an application header – L7 header it is judged what application the packet is.

[0060]

When the address of a packet is in an ad hoc network at this time Since there are few possibilities that it may try to show from the exterior during transmission or may be altered a tunnel is not used but a packet is transmitted to the target node according to the transfer rules of the ad hoc network currently recorded on routing table as it is.

[0061]

When an address is outside an ad hoc network it communicates using the tunnel stretched between the node 2 and the external network 22. When the tunnel for the applications is set up a packet is transmitted using the tunnel. When two or more tunnels are assigned to the applications by procedure such as round-robin (round-robin) one it distributes to the tunnel assigned by the packet unit and transmits to it.

[0062]

The node 2 judges to which application classification of the application DB the application corresponds and chooses the tunnel corresponding to the application classification from the tunnel DB.

[0063]

The node 2 searches the delay which application requires and the tunnel which fulfills both packet loss rates when the tunnel which is satisfied with one of the tunnels hit to

search of a sum total zone (the number of demand zone x sessions) exists assigns one of them to the application and transmits it. When it cannot fill with one or two or more tunnels for which the zone included the largest tunnel are made into 1 set and application is assigned and it transmits to it. Even if it uses two or more when it cannot fill and when it does not hit to search setting out of a tunnel peculiar to the application is not performed but it transmits using a common tunnel.

[0064]

When two communication paths are set to the external network 22 from the node 2 so that it may be shown among a figure if ID of the access node 6 is made into ID-A of the tunnel DB of drawing 4 and the access node 7 is made into the ID-B for example When the application A shown in drawing 12 is VoIP of the application DB of drawing 3 It judges that the course which passes along the access node 6 by a packet judging module in consideration of a time delay packet loss etc. is the optimal communication circuit (when set as the tunnel for VoIP) and data transfer is performed.

[0065]

When the application B is streaming of the application DB of drawing 3 similarly By the packet judging module 38 the optimal communication path is judged to be a course which passes along the access node 7 (when set as the tunnel for streaming) in consideration of a time delay packet loss etc. Transmission of packet data is performed and the optimal communication path can be chosen according to the classification of application and the communication quality of a communication path.

[0066]

When the tunnel for special is not set up to have stated in advance it transmits using a common tunnel and the tunnel for which the above-mentioned applications A and B fulfill most the communication quality demanded respectively is chosen and transmitted.

[0067]

Since the tunnel which secures the quality of the application classification will come to be set up if the user enables it to register into the application DB of the node 2 the application classification used well in drawing 12 The tunnel suitable for the target application classification can be assigned and more efficient communication can be performed.

[0068]

By acquiring the information including the zone and time delay of each course (tunnel) a packet loss rate etc. set up in order to perform communication to an external network from the network of ad hoc mesh shape according to this example of this. Streaming download and voice data a video data text data etc. can choose the suitable course for each communication. Effective use of a zone is attained by dividing the action of a tunnel by communication closed in the communication from a terminal unit to the outside of an ad hoc network and a network.

[0069]

It is not what is restricted to radio although wireless connection constitutes the mesh network from the example of the above-mentioned embodiment. What is necessary is just to carry out two or more owners of the communication path on the mesh network at the time of connecting with the network of the exterior of this mesh network from the terminal unit which carries out direct continuation to a mesh network. Although the network generally formed with the cable has the stable quality of a communication path rather than that of radio. By performing life-and-death surveillance and performance monitoring of a communication path (tunnel) with the application of this invention, also when service of the best effort type in which the course in which a transfer rate changes with the increases in traffic is provided is used, communication quality can be stabilized in the better state.

[0070]

As for this invention, it is needless to say that various composition can be taken in addition to this, without not being restricted to the example of an embodiment mentioned above and deviating from the gist of this invention.

[Brief Description of the Drawings]

[0071]

[Drawing 1] It is a communication network line block diagram of the example of the 1 embodiment of this invention.

[Drawing 2] It is a module block diagram of the node of the example of the 1 embodiment of this invention.

[Drawing 3] It is an explanatory view showing the signal transduction of the access node of the example of the 1 embodiment of this invention and a general node.

[Drawing 4] It is an explanatory view of the default route information distribution of the example of the 1 embodiment of this invention.

[Drawing 5] It is an explanatory view of ad hoc network inner tunnel setting out of the example of the 1 embodiment of this invention.

[Drawing 6] It is an explanatory view of ad hoc network outer tunnel setting out of the example of the 1 embodiment of this invention.

[Drawing 7] It is a tunnel setting-out flow chart of the example of the 1 embodiment of this invention.

[Drawing 8] It is a tunnel addition flow chart of the example of the 1 embodiment of this invention.

[Drawing 9] It is an explanatory view of the data communications of the example of the 1 embodiment of this invention.

[Drawing 10] It is an explanatory view of communication-path selection of the example of the 1 embodiment of this invention.

[Drawing 11] It is an explanatory view of the application database of the example of the 1 embodiment of this invention.

[Drawing 12] It is an explanatory view of the tunnel information database of the

example of the 1 embodiment of this invention.

[Description of Notations]

[0072]

19 --- A terminal unit 2 --- A node (communication-path selecting arrangement) 3 4 5 6 7
--- Node 8 --- A server 10 --- A mesh network 11 12 24 25 --- Tunnel 20 21 22 23 [--- A
quality identification module 34 / --- An application database 35 / --- A tunnel data
information base 38 / --- Packet judging module] --- An external network 31 --- A
tunnel setting-out module 32 --- A node authentication module 33

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[0071]

[Drawing 1] It is a communication network line block diagram of the example of the 1 embodiment of this invention.

[Drawing 2] It is a module block diagram of the node of the example of the 1 embodiment of this invention.

[Drawing 3] It is an explanatory view showing the signal transduction of the access node of the example of the 1 embodiment of this invention and a general node.

[Drawing 4] It is an explanatory view of the default route information distribution of the example of the 1 embodiment of this invention.

[Drawing 5] It is an explanatory view of ad hoc network inner tunnel setting out of the example of the 1 embodiment of this invention.

[Drawing 6] It is an explanatory view of ad hoc network outer tunnel setting out of the example of the 1 embodiment of this invention.

[Drawing 7] It is a tunnel setting-out flow chart of the example of the 1 embodiment of this invention.

[Drawing 8] It is a tunnel addition flow chart of the example of the 1 embodiment of this invention.

[Drawing 9] It is an explanatory view of the data communications of the example of the 1 embodiment of this invention.

[Drawing 10] It is an explanatory view of communication-path selection of the example of the 1 embodiment of this invention.

[Drawing 11] It is an explanatory view of the application database of the example of the 1 embodiment of this invention.

[Drawing 12] It is an explanatory view of the tunnel information database of the example of the 1 embodiment of this invention.

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-72720

(P2005-72720A)

(43) 公開日 平成17年3月17日(2005.3.17)

(51) Int. Cl.⁷

H04L 12/56

H04L 12/28

F I

H04L 12/56

100Z

H04L 12/56

100D

H04L 12/28

307

テーマコード (参考)

5K030

5K033

審査請求 未請求 請求項の数 8 O L (全 16 頁)

(21) 出願番号

特願2003-296657 (P2003-296657)

(22) 出願日

平成15年8月20日 (2003.8.20)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(74) 代理人 100122884

弁理士 角田 芳末

(74) 代理人 100113516

弁理士 磯山 弘信

(72) 発明者 矢野 悠一

東京都品川区北品川6丁目7番35号 ソ
ニー株式会社内

Fターム(参考) 5K030 GA03 HA08 HB16 HD06 JT02

KA05 LB05 LE01 MA04 MB01

MC07

5K033 AA01 CB09 CC01 DA02 DA06

DA19 DB12 EA02 EA07 EC04

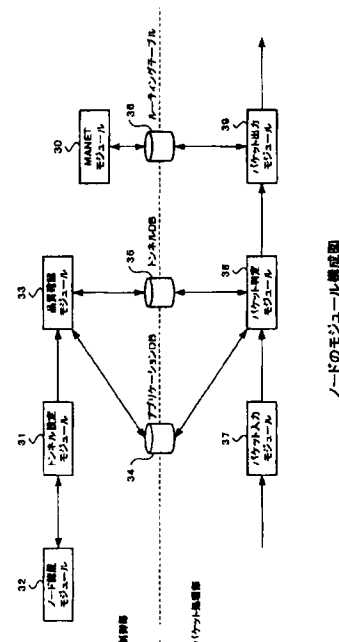
(54) 【発明の名称】 通信ネットワークシステム、通信経路選択装置及び情報通信方法

(57) 【要約】

【課題】 複数のノードが相互に接続して構成される網目状ネットワークに接続している端末装置から外部ネットワークとの通信を行う経路を複数持つ通信ネットワークにおいて、アプリケーションが必要とする品質に見合う最適な経路を利用することができる通信方式を提案することを目的とする。

【解決手段】 複数のノードが相互に接続して構成される網目状ネットワークに接続する端末装置からこの網目状ネットワークを介して外部ネットワークにアクセスする際、網目状ネットワークから外部ネットワークへの通信経路が複数存在する場合に、端末装置と直接接続するノードが、この端末装置から入力されたデータを転送するのに要求される通信品質と各通信経路の通信品質とを照合し、当該データを転送するのに最適な通信経路を選択する。

【選択図】 図2



【特許請求の範囲】**【請求項 1】**

複数のノードが相互に接続して構成される網目状ネットワークに接続する端末装置から前記網目状ネットワークを介して外部ネットワークにアクセスする通信ネットワークシステムであって、

前記網目状ネットワークから外部ネットワークへの通信経路が複数存在する場合に、前記端末装置と直接接続するノードが、前記端末装置から入力されたデータを転送するのに要求される通信品質と各通信経路の通信品質とを照合し、当該データを転送するのに最適な通信経路を選択する通信経路選択手段を有する

ことを特徴とする通信ネットワークシステム。

10

【請求項 2】

請求項 1 記載の通信ネットワークシステムにおいて、

前記通信経路選択手段は、前記端末装置と直接接続するノードと前記外部ネットワークのサーバとの間の通信経路にトンネルを設定するトンネル設定手段と、

予めアプリケーションソフトウェア種別の要求する通信品質を記録するアプリケーション種別品質記録手段と、

各通信経路の通信品質を監視する品質確認手段と、

前記品質確認部の監視により得た品質情報を記録する通信経路品質記録手段と、

一又は複数の端末装置から前記ノードに入力された各データが、前記アプリケーション種別品質記録手段に記録されているいずれのアプリケーションソフトウェア種別に該当するか判断し、前記アプリケーション種別品質記録手段及び前記通信経路品質記録手段に記録されている品質情報を照合し、前記各データの要求する品質を確保する一又は複数の通信経路を指定する経路判別手段と備え、

20

前記指定された通信経路に前記各データを出力する

ことを特徴とする通信ネットワークシステム。

【請求項 3】

請求項 2 記載の通信ネットワークシステムにおいて、

前記トンネル設定手段は、前記トンネルを特定のアプリケーションソフトウェア種別のデータ通信にのみ利用するトンネル、又は任意のアプリケーションソフトウェア種別のデータ通信に利用できるトンネルのいずれかに区分して設定する

30

ことを特徴とする通信ネットワークシステム。

【請求項 4】

複数のノードが相互に接続して構成される網目状ネットワークに接続する端末装置から前記網目状ネットワークを介して外部ネットワークにアクセスする際に前記端末装置と直接接続するノードであり、前記網目状ネットワークから外部ネットワークへの通信経路が複数存在する場合に、前記端末装置から入力されたデータを転送するのに要求される通信品質と各通信経路の通信品質とを照合し、当該データを転送するのに最適な通信経路を選択する

ことを特徴とする通信経路選択装置。

【請求項 5】

40

請求項 4 記載の通信経路選択装置において、

前記通信経路選択手段は、前記端末装置と直接接続するノードと前記外部ネットワークのサーバとの間の通信経路にトンネルを設定するトンネル設定手段と、

予めアプリケーションソフトウェア種別の要求する通信品質を記録するアプリケーション種別品質記録手段と、

各通信経路の通信品質を監視する品質確認手段と、

前記品質確認手段の監視により得た品質情報を記録する通信経路品質記録手段と、

一又は複数の端末装置から前記ノードに入力された各データが、前記アプリケーション種別品質記録手段に記録されているいずれのアプリケーションソフトウェア種別に該当するか判断し、前記アプリケーション種別品質記録部手段及び前記通信経路品質記録手段に

50

記録されている品質情報を照合し、前記各データの要求する品質を確保する一又は複数の通信経路を指定する経路判別手段とを備え、

前記指定された通信経路に前記各データを出力することを特徴とする通信経路選択装置。

【請求項 6】

請求項 5 記載の通信経路選択装置において、

前記トンネル設定手段は、前記トンネルを特定のアプリケーションソフトウェア種別のデータ通信にのみ利用するトンネル、又は任意のアプリケーションソフトウェア種別のデータ通信に利用できるトンネルのいずれかに区分して設定する

ことを特徴とする通信経路選択装置。

10

【請求項 7】

複数のノードが相互に接続して構成される網目状ネットワークに接続する端末装置から前記網目状ネットワークを介して外部ネットワークにアクセスする情報通信方法であって、

前記網目状ネットワークから外部ネットワークへの通信経路が複数存在する場合に、前記通信経路として前記端末装置と直接接続するノードと前記外部ネットワークのサーバとの間の通信経路にトンネルを設定するステップと、

予めアプリケーションソフトウェア種別の要求する通信品質を記録するステップと、

前記通信経路に設定したトンネルの通信品質を監視するステップと、

監視により得られた前記トンネルの品質情報を記録するステップと、

20

前記端末装置から前記ノードに入力された各データが、前記アプリケーション種別品質記録手段に記録されているいずれのアプリケーションソフトウェア種別に該当するか判断し、前記アプリケーション種別の要求する通信品質と前記トンネルの通信品質を照合し、前記データの要求する通信品質を確保する一又は複数の通信経路を指定するステップと、

前記指定された通信経路に前記データを出力するステップとを備える

ことを特徴とする情報通信方法。

【請求項 8】

請求項 7 記載の情報通信方法において、

前記トンネルを設定するステップにおいて、前記トンネルを特定のアプリケーションソフトウェア種別のデータ通信にのみ利用するトンネル、又は任意のアプリケーションソフトウェア種別のデータ通信に利用できるトンネルのいずれかに区分して設定する

30

ことを特徴とする情報通信方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、例えば網目状に接続されたノードで構成されるネットワークに加入する端末装置から外部ネットワーク上のサーバにアクセスして情報通信を行う通信ネットワークシステム、通信経路選択装置及び情報通信方法に関する。

【背景技術】

【0002】

近年の無線技術のひとつにアドホックネットワークがあるが、このアドホックネットワークは、多数の端末をアクセスポイントの介在なしに相互に接続する形態(マルチホップ通信)を取っており、無線技術を用い網目状にネットワークを形成して複数経路の利用を可能とする。このため、アドホックネットワークでは基地局やアクセスポイントが不要となり、このようなインフラを持たない場所で安価にネットワークを構築することができ、ある限られた域内での簡易なネットワークの構築の手段として有効である。

40

【0003】

しかし、アドホックネットワークは、各ノードが自律的に無線接続してネットワークの構成を行うため、有線ネットワークと違い、例えば通信レートが時々刻々と変化するなど、技術的課題が残されており通信経路の定常的な品質を確保することは困難である。

50

【0004】

その対策の一つとして、ネットワーク内でのデータの通信レートに応じて、アプリケーションソフトウェア（以下、アプリケーションと称する。）の起動を制御し、常に良好な動作状態でアプリケーションを動作させるようにしたものに、例えば、ネットワーク内でのクライアント端末とホスト端末との間のデータ通信レートを測定し、その測定履歴に基づいて、その通信レートがクライアント端末の所定アプリケーションを正常に動作させる通信レートに満たないと判断された場合、クライアント端末の所定アプリケーションの起動を制限するようにした技術がある（例えば、特許文献1参照。）。

【特許文献1】特開2003-122672号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

しかしながら、特許文献1に記載のものは、ネットワーク内の対象とする端末間の通信回線の通信レートを測定して得られる通信レートに応じて、クライアント端末において起動して正常に動作させることのできるアプリケーションのみ起動できるよう制御するものであり、アプリケーションの要求する通信レートが得られない場合は目的のアプリケーションを起動することができないという不都合があった。

【0006】

また、アドホックネットワークでは、各ノードにとっての最適経路のみを計算し、その経路を利用して通信を行う。しかしその場合、アドホックネットワーク外へアクセスするノードが複数存在したとしても一般のTCP/IP（Transmission Control Protocol/Internet Protocol）を利用する現状では、アプリケーションソフトウェア等による1つのセッションが利用可能なのは1つの経路のみとなり、同一セッションのときは分散できないため、経路が複数ある利点を生かすことができていないという不都合があった。

【0007】

斯かる点に鑑み、本発明は、複数のノードが相互に接続して構成される網目状ネットワークに接続している端末装置から外部ネットワークとの通信を行う経路を複数持つ通信ネットワークにおいて、アプリケーションが必要とする品質に見合う最適な経路を利用することができる通信方式を提案することを目的とする。

【課題を解決するための手段】

【0008】

上記課題を解決し、目的を達成するため、本発明は、複数のノードが相互に接続して構成される網目状ネットワークに接続する端末装置からこの網目状ネットワークを介して外部ネットワークにアクセスする際、網目状ネットワークから外部ネットワークへの通信経路が複数存在する場合に、端末装置と直接接続するノードが、この端末装置から入力されたデータを転送するのに要求される通信品質と各通信経路の通信品質とを照合し、当該データを転送するのに最適な通信経路を選択するようにしたものであり、より具体的には、端末装置と直接接続するノードと外部ネットワークのサーバとの間の通信経路にトンネルを設定するトンネル設定手段と、予めアプリケーションソフトウェア種別の要求する通信品質を記録するアプリケーション種別品質記録手段と、各通信経路の通信品質を監視する品質確認手段と、この品質確認手段の監視により得た品質情報を記録する通信経路品質記録手段と、一又は複数の端末装置からこのノードに入力された各データが、前記アプリケーション種別品質記録手段に記録されているいずれのアプリケーションソフトウェア種別に該当するか判断し、このアプリケーション種別品質記録手段及びこの通信経路品質記録手段に記録されている品質情報を照合し、各データの要求する品質を確保する一又は複数の通信経路を指定する経路判別手段と備え、この指定された通信経路に各データを出力することを特徴とする。

【0009】

斯かる本発明によれば、網目状ネットワークから外部ネットワークへの通信経路が複数存在する場合に、端末装置と直接接続するノードが、その端末装置から入力されたデータ

10

20

30

40

50

を転送するのに要求される通信品質と各通信経路を監視することにより得た通信品質とを照合することで、対象とするデータを転送するのに必要とされる品質を持つ通信経路を選択し、最適な経路を利用する。

【0010】

また本発明は、上述トンネル設定手段は、トンネルを特定のアプリケーションソフトウェア種別のデータ通信にのみ利用するトンネル、又は任意のアプリケーションソフトウェア種別のデータ通信に利用できるトンネルのいずれかに区分して設定することを特徴とする。

【0011】

斯かる本発明において、トンネルを設定する際にトンネルをある特定のアプリケーションソフトウェアに利用する固定用、又は任意のアプリケーションソフトウェアに利用できる一般用のいずれかに区分することで、入力されたデータのアプリケーションソフトウェア種別を特定するだけで、トンネル（通信経路）をアプリケーションソフトウェア種別の要求する品質に合わせて適切に割り当てることができる。

【発明の効果】

【0012】

斯かる本発明によれば、例えばアドホックな網目状のネットワークから外部ネットワークへの通信を行うために設定した各経路（トンネル）の帯域や遅延時間、パケット損失率等の通信品質に関する情報を得ることで、端末装置から入力されるストリーミングやダウンロードのデータ、音声データ、動画データ、テキストデータなど、各通信に適切な経路を選択することができ、各経路の帯域の有効利用が可能となる。したがって、網目状ネットワークから外部ネットワークへアクセスする際の定常的な通信品質を確保することができる。

【0013】

また、トンネルを特定のアプリケーションソフトウェア用、又は任意のアプリケーションソフトウェアに利用できる一般用に区分して設定することで、入力されたデータのアプリケーションソフトウェア種別を特定するだけで、トンネル（通信経路）をアプリケーションソフトウェア種別の要求する品質に合わせて適切に割り当てることができ、より効率よく各経路の帯域を有効利用できる。

【発明を実施するための最良の形態】

【0014】

以下、図1～図12を参照して、本発明の一実施の形態の例について説明する。

本例は、ゲートウェイ機能を備えるノード間をアドホックに結合することで通信を実現する自立分散型ネットワークに加入している端末装置から、インターネット等外部ネットワークにアクセスする場合に適用した例としてあり、この例のアドホックな通信ネットワーク自体は、MANET（Mobile Ad-hoc Networks）等既存の技術を用いていわゆる略網目状（メッシュ）のネットワークを構成している。

【0015】

図1に、本例の通信ネットワークシステムの全体図を示す。

1はゲートウェイ機能を備えたノード2～7より構成されるアドホックネットワークに接続可能な端末装置である。ノード2～7は周囲に存在する複数のノードと相互接続し、この例ではIP（Internet Protocol）によりネットワーク（以下、NWと称する。）10を形成する。8はインターネット等の外部ネットワーク（以下、外部NWと称する。）20上に設けられ、アドホックネットワーク上のノード6又は7からの通信要求及びデータを受信するサーバである。このサーバ8はNW10内のノードと後述するトンネルを形成するトンネルサーバとしても機能する。9はサーバ8と通信可能に接続されている端末装置である。この例では、アクセス回線に接続するノード6、7がアクセスノード、その他は一般ノードとなっている。

【0016】

図2に、本例の網目状ネットワークを形成するノードのソフトウェアモジュール構成を

10

20

30

40

50

示す。

図中示すように、MANETモジュール30、トンネル設定モジュール31、ノード認証モジュール32、品質確認モジュール33、アプリケーションデータベース（以下、アプリケーションDBと称する。）34、トンネル情報データベース（以下、トンネルDBと称する。）35、ルーティングテーブル36、パケット入力モジュール37、パケット判定モジュール38及びパケット出力モジュール39により構成され、図示しないROM（Read Only Memory）に格納されているものとする。

【0017】

トンネル設定モジュール31及びノード認証モジュール32はトンネル設定手段として機能し、トンネル設定を行う際に必要となるトンネル形成情報、トンネル設定要求、ノード認証等を送受信する。そして、品質確認手段として機能する品質確認モジュール33は、トンネル設定モジュール31からトンネル設定情報を受信し、例えば端末装置と直接接続するノード2のような一般ノードにおける品質確認モジュール33は、実際に接続を設定したトンネルの通信品質を定期的に監視して、その品質情報をトンネルDB35に登録するとともに、後述するアプリケーションDB34に登録されたアプリケーション種別の要求する通信品質との比較等を行う。

【0018】

アプリケーションDB34はアプリケーションソフトウェア（以下、アプリケーションと称する。）種別の要求する通信品質を記録するアプリケーション種別品質記録手段として機能し、ノードを通るデータが要求する品質をアプリケーション毎に整理して格納するデータベースであり、例えば後述の図11に示すように、アプリケーション種別、DSCP（DiffServ Code Point）、遅延時間、パケット損失率、伝送帯域、セッション数等の情報が登録されている。このセッション数は、例えば図1のノード2に複数の端末装置を接続し通信を行うような場合を想定したときに、同一アプリケーション種別においてノード2が同時に制御可能なセッション数を表す。

【0019】

トンネルDB35は通信経路品質記録手段として機能し、品質確認モジュール33により設定されたトンネルを定常的に監視して得られる品質情報、例えば後述の図12に示すように、経路上のアクセスノードのID、IPアドレス、遅延時間、パケット損失率、割当帯域、通信品質の測定時刻等の情報が格納されている。

【0020】

ルーティングテーブル36は、一般的なルーティングとしてこの例ではアドホックネットワーク内の経路表や設定したトンネルの経路表を保持する。

【0021】

MANETモジュール30は、隣接するノードと自立的にネットワークを構築するとともに、例えば、上述ルーティングテーブル36の経路表に基づいてIETF（Internet Engineering Task Force）のワーキンググループ（WG）で種々提案されているようなMANETルーティングプロトコルによる通信を行う。

【0022】

パケット入力モジュール37は、一般ノード側ではLAN（Local Area Network）やWAN（Wide Area Network）などから入力されてきたパケットの処理を行う。アクセスノードでも同様である。パケット入力モジュール37は外部から受信したパケットをパケット判定モジュール38に供給する。

【0023】

パケット判定モジュール38は経路判別手段として機能し、アプリケーションDB34及びトンネルDB35を照合してパケット入力モジュール37で抽出したパケットの情報をどのトンネル（通信経路）を通して外部ネットワークに転送するかを指定しパケット出力モジュール39に送信する。パケット出力モジュール39は、パケット判定モジュール38で指定された経路にパケットを出力する。

【0024】

10

20

30

40

50

各ノードのこれらのモジュールは、ノード認証モジュール 3 2、トンネル設定モジュール 3 1、品質確認モジュール 3 3 及び M A N E T モジュール 3 0 により制御部を構成し、また、パケット入力モジュール 3 7、パケット判定モジュール 3 8 及びパケット出力モジュール 3 9 によりパケット処理部を構成し、制御部及びパケット処理部が、アプリケーションデータベース 3 4、トンネル情報データベース 3 5 とルーティングテーブル 3 6 に格納された情報に応じて、パケットの適切な通信制御を行う。

【0025】

上述の如く構成される各ノードの一般ノードにおける主な機能は、次のようなものである。

1. 既存技術を用いて自立的にアドホックネットワークを構築する。 10
2. アクセスノードからのブロードキャストを受信し、その情報を元にトンネルの設定を行う。
3. アクセスノードにトンネリングによる接続要求を行う。
4. 接続したトンネルの品質を定期的に監視する。
5. 入出力されるアプリケーションの要求する品質が格納されている D B を保持する。
6. で監視しているトンネルの品質が格納されている D B を保持する。
7. アドホックネットワークとトンネルの経路情報を保持する。
8. L A N や W A N など、他のノードから入力されるパケットの処理を行う。
9. パケット入力モジュールで抽出したパケットの情報を元に、パケットの転送先を決定 20 する。
10. パケット判定モジュールで指定された経路にパケットを出力する。

【0026】

また、アクセスノードにおける主な機能は、次のようなものである。

1. 既存技術を用いて自立的にアドホックネットワークを構築する。
2. 自身が接続しているアクセス回線の情報と、各ノードに対して許容する通信帯域をブロードキャストなどの手法によりアドホックネットワーク内に広告する。
3. 一般ノードからの接続要求の認証を行う。
4. アドホックネットワークとトンネルの経路情報を保持する。
5. L A N や W A N など、他のノードから入力されるパケットの処理を行う。
6. パケット入力モジュールで抽出したパケットの情報を元に、パケットの転送先を決定 30 する。
7. パケット判定モジュールで指定された経路にパケットを出力する。

【0027】

図 3 を参照して、ネットワーク内のアクセスノードと一般ノード間で行われる情報伝達を説明する。

まず、アクセスノードはトンネル設定モジュール 3 1 a より不特定の一般ノードに対し、トンネル形成情報として利用されるデフォルトルート（デフォルト通信経路）情報を定期的にブロードキャスト（配布）する。一般ノードはトンネル設定モジュール 3 1 a にてデフォルトルート情報を受信し、その情報を基にアクセスノードに対しトンネリングによる接続（トンネル設定）要求を行う。 40

【0028】

アクセスノードは一般ノードからのトンネル設定要求に応じ、トンネル設定モジュール 3 1 b がノード認証モジュール 3 2 b にノード認証要求信号を出力する。ノード認証モジュール 3 2 b はトンネル設定を要求した一般ノードに対しノード認証する旨を通知する。ノード認証通知を受け取ったトンネル設定モジュール 3 2 a は、例えば明らかにトンネルの帯域が狭かったりパケット損失率が大きい等の問題が見られなければ、アクセスノードへノード認証に対する応答をする。

【0029】

また、アクセスノードはノード認証モジュール 3 2 b にて一般ノードからのノード認証の応答を受信して、トンネル設定モジュール 3 1 b へトンネル設定許可信号を供給し、ト 50

ンネル設定モジュール 3 1 b から一般ノードへトンネル設定情報を送信する。

【0030】

そして、一般ノードではトンネル設定モジュール 3 1 a にてトンネル設定情報を受信し図 2 に示したルーティングテーブル 3 6 に登録するとともに、品質確認モジュール 3 3 a はこのトンネル設定情報を基に定常的にトンネルの品質監視を行い、そのトンネルの品質をトンネル DB 3 5 a にトンネル情報として登録する。そして、後述するが品質確認モジュール 3 3 a はアプリケーション DB 3 4 a に登録されているアプリケーション情報を参照して登録されているトンネル情報とアプリケーション種別の要求する品質との整合性を判断し、Q o S (Quality of Service) を実現する。

【0031】

次に、本例の通信ネットワークシステムのトンネル設定について、図 4 ～ 6 の説明図、図 7, 8 のフローチャートを参照して説明する。

まず、各ノードは、既存技術を用いて自立的にアドホックなネットワーク (NW) 1 0 を構築する。各ノードは、特定のアプリケーションについて、I P / I C M P (Internet Control Message Protocol) ヘッダなどの O S I 参照モデルでのレイヤー 3 ヘッダ、及び T C P (Transmission Control Protocol) / U D P (User Datagram Protocol) ヘッダなどのレイヤー 4 ヘッダの情報、並びにそのアプリケーションが要求する遅延・帯域・パケット損失率などの情報を、図 2 に示したようにデータベースとして保持する。

【0032】

図 4 にトンネル設定を行う際のデフォルトルート情報配布の説明図を示す。外部 NW 2 0 に接続しているアクセスノード 6, 7 は、NW 1 0 外と接続している旨をトンネル形成情報として利用されるデフォルトルート (デフォルト通信経路) 情報を、隣接するノードにブロードキャスト (配布) する (ステップ S 1)。

【0033】

この例では、ノード 2 は、図 4 に示すようなノード 6, 3 を通る経路とノード 7, 4 を通る経路のトンネル形成情報を受信する。このトンネル形成情報の基となるデフォルト通信経路情報は NW 1 0 上を定常的にブロードキャストされており、端末装置 1 が NW 1 0 に接続したときに受信され、通常の I P 層でのやり取り、あるいはアプリケーション層でのやり取り、いずれでも構わない。

【0034】

図 5 は、本例のアドホックネットワーク内トンネル設定の説明図である。ノード 2 は、受け取ったデフォルト通信経路情報に従って、アクセスノード 6, 7 に対し、トンネル設定をリクエストする (ステップ S 2)。トンネルの設定に関しては既存の技術が用いられる。NW 1 0 内での盗聴等を防ぐため、例えば、I P - i n - I P (R F C 1 8 5 3) や G R E (R F C 1 7 0 1) よりも、I P s e c (Security Architecture for Internet Protocol) のトンネルモードの利用がより好ましい。

【0035】

アクセスノード 6, 7 は、リクエストしてきたノード 2 の認証を行うか否かを判断し (ステップ S 3)、接続対象として不適切であると判断したならば認証を拒否し、所定の指定回数認証を失敗したかどうかを判別し (ステップ S 4)、指定回数認証を失敗していないのであればステップ S 2 の処理に戻り、トンネルリクエストを繰り返す。指定回数認証を失敗したときはトンネル設定処理を終了する。アクセスノード 6, 7 はノード 2 が接続対象として適切であると判断し認証が通った場合にノード 2 へトンネルの情報を送信する (ステップ S 5)。

【0036】

ノード 2 は、アクセスノード 6, 7 から受信したトンネル情報がノード 2 にとって有効なものであるかどうかを判断し (ステップ S 6)、有効でない場合はトンネル設定処理を終了する。有効であると判断した場合、ノード 2 は受信したトンネル情報を基に、ノード 2 とノード 6 及びノード 7 の間でそれぞれトンネルを設定する (ステップ S 7)。

【0037】

10

20

30

40

50

図6は、本例のメッシュネットワーク外トンネル設定の説明図である。端末装置1と接続されたノード2とアクセスノード6、7との間に張られたトンネル11、12を利用し、さらに外部ネットワーク20上のサーバ8との間にトンネルを設定する。ノード2は、デフォルト通信経路を設定した各トンネル11、12から、NW10外のサーバ8に向けてトンネル接続を要求する。この際、サーバ8による認証が行われる。ノードの識別には、該当ノードの機器IDやNW10内のIPアドレスが送信され、認証に利用される。

【0038】

また、トンネルサーバ8は通常の認証処理に加え、以下の登録を行う。ノード2に対し使用されるIPアドレスは通信経路の分複数あるが、それらを登録しておくことで、複数のトンネルからの通信を1つのフロー(flow)として識別する。トンネルサーバ8は、ノード2との間に張られた複数のトンネルから届くパケットのヘッダを外し、上述IPアドレスに基づいて1つのフローに戻す。

【0039】

サーバ8はノード2からのトンネル設定要求に際し、接続対象として不適切であると判断したならば認証を拒否する。また、接続対象として問題がなければ適切であると判断し認証を許可する旨をノード2に返信し、トンネル11を利用してノード2とサーバ8との間でトンネルを設定する。同様に、NW10内に設定したトンネル12を利用してノード2とサーバ8とのトンネルを設定する。設定されたトンネル情報は、トンネルDBに登録される。図6の例では、NW10の端末装置1から外部NW20のサーバ8にアクセス可能なトンネル(通信経路)が2つ存在する。

【0040】

次に、設定したトンネルの品質監視を行う定常的トンネル監視フェーズについて説明する。

まず、ノード2はトンネルを設定するとその新規に設定したトンネルの情報をトンネルDBに追加登録する(ステップS8)。このときのトンネル追加フローについて、図8のフローチャートを参照して説明する。

【0041】

ノード2はアプリケーションDBに、例えばストリーミングデータ等の特殊な転送ルールを要求するアプリケーションが存在するか否かを判断する。ノードは、アプリケーションDBとトンネルDBを比較し、個別アプリケーション種別の要求する通信品質を確保できるトンネルが存在するかを確認する(ステップS21)。特殊な転送ルールが存在しない場合には、新規トンネルを一般トンネルに追加する(ステップS22)。ここで一般トンネルとは、特定のアプリケーション用途の通信に限定されない、他目的に利用されるトンネルである。また、特殊用トンネルとは特定アプリケーション用途にのみ使用するトンネルを指すものとする。

【0042】

次に、特殊な転送ルールを要求するアプリケーションがアプリケーションDBに存在する場合、新規設定したトンネルを含めトンネルDBに登録されているトンネルの中に、この特殊な転送ルールに最適なトンネルが存在するか否かを判断し(ステップS23)、存在しない場合新規トンネルを一般トンネルに追加登録する(ステップS24)。

【0043】

ステップS23の処理で特殊な転送ルールに対し最適なトンネルが存在する場合、まず、それが一本のときはその一本のトンネルが新規トンネルか否かを判断する(ステップS25)。新規トンネルであった場合には、その新規トンネルを専ら特殊な転送ルールのアプリケーションの通信に限定した特殊用(個別用)トンネルに設定しトンネルDBに登録する(ステップS26)。新規トンネルでない場合は、新規トンネルを一般トンネルに、該当トンネルを特殊用トンネルに設定、登録する(ステップS27)。

【0044】

また、ステップS23の処理で特殊な転送ルールに対しトンネルDBに最適なトンネルが存在する場合、まず、それが複数本のときはその複数本のトンネルの中に新規トンネル

10

20

30

40

50

が含まれるか否かを判断する（ステップ S 2 8）。新規トンネルが含まれる場合には、その新規トンネルを含むトンネル群を専ら特殊な転送ルールのアプリケーションの通信に限定した特殊用トンネルに設定、登録し（ステップ S 2 9）、新規トンネルを含まない場合は、新規トンネルを一般トンネルに、該当トンネル群を特殊用トンネルに設定、登録する（ステップ S 3 0）。

【0045】

このように、トンネルを予め一般用及び特殊用に割り当ててデータベースに登録することで、端末装置からノードに入力されたデータのアプリケーションが要求する品質に応じて即座に適切なトンネル（通信経路）を選択することができる。

【0046】

そして、ノード 2 の品質確認モジュールからサーバ 8 との間に張られたトンネルに対し、例えば 1 秒間隔などで定期的に死活確認・品質情報要求用のビーコンを送信し（ステップ S 9）、サーバ 8 のトンネル通信品質応答モジュール（図示せず）から応答される、遅延時間、パケット損失率等の品質情報を収集しトンネル DB に記録する。このとき、ビーコンの送信に対してトンネルからの反応があるか否かを判断し（ステップ S 1 0）、反応があり品質情報要求に対する応答が返ってきた場合には、返信されてきたトンネル品質情報をデータベースに反映するとともに、図 1 2 の測定時刻を基に設定した有効期間を更新し（ステップ S 1 1）、ステップ S 8 の処理に移行して定常的トンネル監視を続ける。

【0047】

有効期間内にトンネルからの反応がない場合には、そのトンネルの情報をトンネル DB から削除し切断する（ステップ S 1 2）。例えば、所定回数ビーコンを送信して応答がなかったら通信経路ダウンと判断してそのトンネルをトンネル DB から削除し切断したり、或いは、トンネルの品質が一定の基準以下になった場合には、死活監視で該当しなくてもトンネルを切断するようにしてもよい。これらトンネルの品質情報をデータベースに保持する。

【0048】

尚、ステップ S 8 の一連のトンネル追加フローにおいて、全ての新規に設定するトンネルをまず一般用トンネルとして登録するという方法が考えられる。即ち、一般ノードは、一番初めに設定したトンネルを一般アプリケーション用のトンネルとして登録し、アプリケーション固有のトンネルが設定されるまでは、一般用トンネルを用いて全てのアプリケーションを転送する。以降、新規トンネルが設定された場合、そのトンネルは最初は一般トンネルとして追加・登録し、定常的トンネル監視の過程で、時々刻々と変化するトンネルの通信品質に応じて随時用途の変更を行うようにする。

【0049】

ノードは、アプリケーション DB とトンネル DB を比較し、個別アプリケーション種別の要求する通信品質を確保できるトンネルが存在するか定期的に確認する。1 本のトンネルで品質を確保できない場合は、確保できるまでそのアプリケーションは一般用トンネルを用いて転送される。個別用トンネルは、一般用トンネルが残り 1 本になるまで追加することができる。一般用トンネルを最低 1 本残しておくことで、全てのアプリケーションに対応することができ、アプリケーション種別に依っては対応するトンネルがなく通信できないという事態を回避する。

【0050】

図 9 は、本例の通信ネットワークシステムが NW 1 0 に接続する端末装置 1 が外部ネットワーク 2 0 の端末装置 9 と通信する場合の一例を示し、以下のようなパケットフォーマット形式で実装することができる。

【0051】

この例は、I P s e c（トンネルモード）+ N A T（Network Address Translation）トラバーサルの実用形態であるが、このとき、サーバ 8 は下記の機能を果たす。

- ・機器 I D を見て、適切な I P アドレスに変換する機能を持つ。
- ・適切な時間キュー方式（queue）にバッファし、できるだけ T C P のシーケンス番号順

10

20

30

40

50

に送出する。

・UDPの場合はそのまま送出する。

【0052】

それぞれの機器にIPアドレスを割り当て、例えば、端末装置1はIPアドレス「IP-1」及び機器ID「E-ID」、通信経路選択装置であるノード2はNATによりIPアドレス「IP-Z」とする。また、アクセス回路に接続するノード6, 7は、それぞれNW10側よりNATによるIPアドレス「IP-A」、「IP-B」及び外部NW20よりNAPT (Network Address Port Translation) によるIPアドレス「IP-1」、「IP-2」とする。さらにまた、サーバ8はNAPTによるIPアドレス「IP-3」、端末装置9はIPアドレス「IP-4」とする。

10

【0053】

ノード2からサーバ8へ複数のトンネルが張られている場合、ノード2は、端末装置1から発信されるデータを、ラウンドロビン (round-robin) などの方式により複数のIPアドレスを割り当て、1パケット単位で自身が利用可能なトンネルに対し転送する。このとき端末装置1からノード2への通信のパケット情報は、「DATA」「TCPヘッダ (z→4)」のみである。そして、ノード2によりトンネル11, 12の2つの通信経路に分散して転送されると、ノード2からノード6及びノード7への通信のパケット情報は、「DATA」「IPヘッダ」「IPsecヘッダ」「トンネルIPヘッダ」となり、トンネル11, 12の両端のノードのIPアドレス情報を表す「IPsecヘッダ」とトンネル内を送信するための「トンネルIPヘッダ」が付加される。

20

【0054】

さらに、ノード6から外部NW20内のサーバ8へ転送されると、その通信パケット情報は、NW10上でトンネル11, 12を利用して送信する情報が消え、ここではNW10とNW20間の通信のプロトコルとしてUDPを用いていることで「UDPヘッダ」がそれぞれ付加されている。サーバ8は、機器IDとTCPヘッダに基づいてノード6, 7から送信されたパケットの出所が同一のノード2からのものであると判断して、パケット単位に分散された情報の再構成を行う。このとき、この例では、UDPによる通信であるので、ラウンドトリップ時間を考慮して再構成し、「DATA」「TCPヘッダ (3→4)」の情報として、サーバ8から端末装置9へパケットを一つの通信情報に再構成したものを転送することで、端末装置9は、端末装置1からのデータを受け取ることができる。

30

【0055】

サーバ8は、単一のノード2から複数のトンネルが張られている時、該当ノード2の機器IDやNW10内のIPアドレスによって同一のノード2からの異なるトンネルであることを認識し、複数のトンネル経由で転送される同一のノードからのパケットをひとつの通信に再構成する。例えば、TCPの場合はシーケンス番号で、UDPの場合はラウンドトリップ時間 (RTT: Round Trip Time) の差分を利用して正しい順序での再構成を行い、外部へ転送する。

【0056】

以上の仕組みを実装することで、ノード2に接続する端末装置は、隣接するノードとの経路を複数利用することができ、1つのセッションを複数帯域に分散させることが可能であるため、一つあたりの通信経路にかかる負担を軽減し、通信速度の上限を大幅に向上することができる。さらに、複数セッションを同時に通信することができる。

40

【0057】

本例の通信ネットワークシステムにおいて端末装置からデータが入力されたときの通信経路の選択について、図12を参照して説明する。この図12は、図1、図6～図8と比較すると、アドホックネットワーク上のアクセスノード6, 7はそれぞれ外部ネットワーク21, 23を経由してネットワーク22の図示しないサーバと接続するとともにそれぞれトンネル24, 25を設定し、端末装置9と通信するようにしている点が相違しているがその他は同様の構成である。

【0058】

50

端末装置 1 又は 9 から見れば、トンネル 1 1 及び 2 4、若しくはトンネル 1 2 及び 2 5 を経由して、あたかも各端末装置からはデータがノード 2 とネットワーク 2 2 上の図示しないサーバと間を直接通信されているように見えるが、実際には、それぞれ太線部を経由して端末装置 1 と端末装置 9 間のデータ通信が行われる。

【0059】

端末装置 1 と直接接続しているノード 2 は、端末装置 1 からデータ（パケット）が入力されてきたときに、IP/ICMP ヘッダなどのレイヤー 3 ヘッダ、及び TCP/UDP ヘッダなどのレイヤー 4 ヘッダ、アプリケーションヘッダなどのレイヤー L5～L7 ヘッダを参照し、そのパケットが何のアプリケーションなのかを判断する。

【0060】

このとき、パケットの宛先がアドホックネットワーク内の場合は、外部から転送中に覗き見られたり改ざんされたりする恐れが少ないので、トンネルを利用せず、そのままルーティングテーブルに記録されているアドホックネットワークの転送ルールに従ってパケットを目的のノードまで転送する。

【0061】

宛先がアドホックネットワーク外の場合は、ノード 2 と外部ネットワーク 2 2 との間に張られたトンネルを利用して通信を行う。そのアプリケーション用のトンネルが設定されている場合はそのトンネルを用いてパケットを転送する。複数のトンネルがそのアプリケーション用に割り当てられている場合は、ラウンドロビン（round-robin）などの手順により、パケット単位で割り当てたトンネルに振り分けて転送する。

【0062】

ノード 2 はそのアプリケーションがアプリケーション DB のどのアプリケーション種別に該当するかを判断し、トンネル DB からそのアプリケーション種別に対応したトンネルを選択する。

【0063】

ノード 2 は、アプリケーションの要求する遅延とパケット損失率の両方を満たすトンネルを検索し、検索にヒットしたトンネルのうち、1 本で合計帯域（要求帯域×セッション数）を満足するトンネルが存在する場合はその 1 本をそのアプリケーションに割り当てて転送する。1 本で満たすことができない場合は、帯域が最も広いトンネルを含めた複数本のトンネルを 1 組としてアプリケーションに割り当てを行い転送する。複数本を用いても満たすことができない場合、及び検索にヒットしなかった場合はそのアプリケーション固有のトンネルの設定は行わず、一般トンネルを用いて転送する。

【0064】

図中示すように、ノード 2 から外部ネットワーク 2 2 へ 2 つの通信経路が設定されている場合、例えば、アクセスノード 6 の ID を図 4 のトンネル DB の ID-A、アクセスノード 7 を同 ID-B とすると、図 1 2 に示すアプリケーション A が図 3 のアプリケーション DB の VOIP であるとき、パケット判定モジュールでは遅延時間、パケット損失等を考慮してアクセスノード 6 を通る経路（VOIP 用トンネルに設定されているとき）が最適通信回路であると判断して、データ転送を行う。

【0065】

また同様に、アプリケーション B が図 3 のアプリケーション DB のストリーミングであるとき、パケット判定モジュール 3 8 では遅延時間、パケット損失等を考慮して最適な通信経路をアクセスノード 7 を通る経路（ストリーミング用トンネルに設定されているとき）であると判断して、パケットデータの転送が行われ、アプリケーションの種別、通信経路の通信品質に応じて、最適な通信経路を選択することができる。

【0066】

先にも述べたように、特殊用トンネルが設定されていない場合には、一般トンネルを利用して転送し、上述アプリケーション A 及び B がそれぞれ要求する通信品質を最も満たしているトンネルを選択し転送するようにする。

【0067】

10

20

30

40

50

また、図 12 において、よく利用するアプリケーション種別を利用者がノード 2 のアプリケーション DB に登録できるようにしておくと、そのアプリケーション種別の品質を確保するトンネルが設定されるようになるので、目的のアプリケーション種別に合ったトンネルを割り当てることができより効率的な通信を行うことができる。

【0068】

斯かる本例によれば、アドホックな網目状のネットワークから外部ネットワークへの通信を行うために設定した各経路（トンネル）の帯域や遅延時間、パケット損失率等の情報を得ることで、ストリーミングやダウンロード、音声データ、動画データ、テキストデータなど、各通信に適切な経路を選択することができる。さらに、端末装置からアドホックなネットワーク外への通信及びネットワーク内に閉じた通信によってトンネルの挙動を分けることによって、帯域の有効利用が可能となる。

10

【0069】

尚、上述実施の形態の例では、無線接続により網目状ネットワークを構成しているが無線に限るものではなく、また、網目状ネットワークに直接接続する端末装置からこの網目状ネットワークの外部のネットワークに接続する際の網目状ネットワーク上での通信経路を複数有するものであればよい。一般に有線で形成されたネットワークは無線のそれよりも通信経路の品質が安定しているが、トラフィックの増加によって転送レートが変化するような経路が設けられているベストエフォート型のサービスを用いている場合にも本発明を適用して通信経路（トンネル）の死活監視・品質監視を行うことで、通信品質をより良好な状態で安定させることができる。

20

【0070】

また、本発明は上述した実施の形態の例に限られるものではなく、本発明の要旨を逸脱することなくその他種々の構成を取り得ることは勿論である。

【図面の簡単な説明】

【0071】

【図 1】 本発明の一実施の形態の例の通信ネットワーク構成図である。

【図 2】 本発明の一実施の形態の例のノードのモジュール構成図である。

【図 3】 本発明の一実施の形態の例のアクセスノードと一般ノードの情報伝達を示す説明図である。

【図 4】 本発明の一実施の形態の例のデフォルトルート情報配布の説明図である。

30

【図 5】 本発明の一実施の形態の例のアドホックネットワーク内トンネル設定の説明図である。

【図 6】 本発明の一実施の形態の例のアドホックネットワーク外トンネル設定の説明図である

【図 7】 本発明の一実施の形態の例のトンネル設定フローチャートである。

【図 8】 本発明の一実施の形態の例のトンネル追加フローチャートである

【図 9】 本発明の一実施の形態の例のデータ通信の説明図である。

【図 10】 本発明の一実施の形態の例の通信経路選択の説明図である。

【図 11】 本発明の一実施の形態の例のアプリケーションデータベースの説明図である。

【図 12】 本発明の一実施の形態の例のトンネル情報データベースの説明図である。

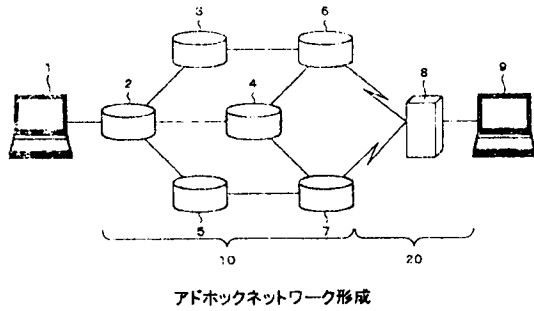
40

【符号の説明】

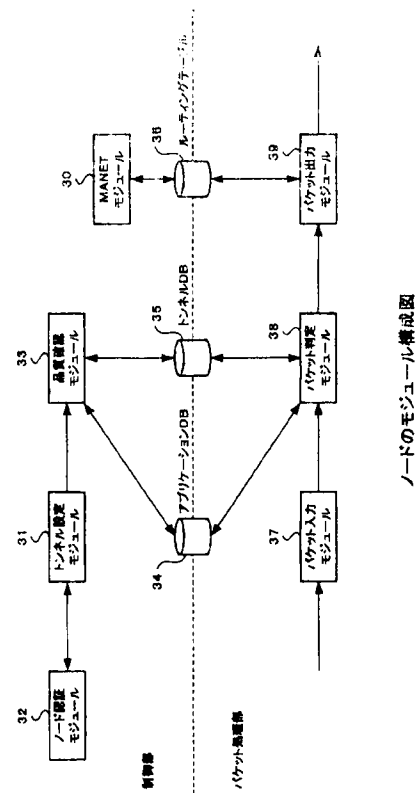
【0072】

1, 9…端末装置、2…ノード（通信経路選択装置）、3, 4, 5, 6, 7…ノード、8…サーバ、10…網目状ネットワーク、11, 12, 24, 25…トンネル、20, 21, 22, 23…外部ネットワーク、31…トンネル設定モジュール、32…ノード認証モジュール、33…品質確認モジュール、34…アプリケーションデータベース、35…トンネルデータ情報ベース、38…パケット判定モジュール

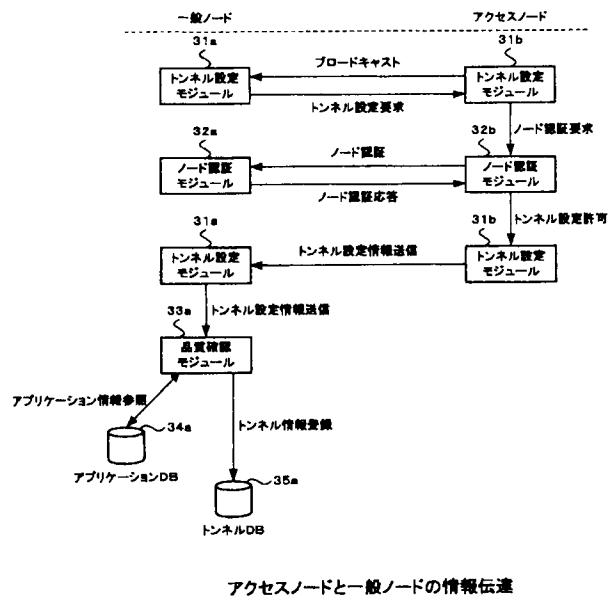
【図 1】



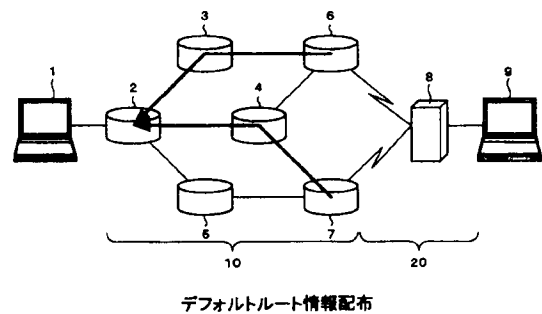
【図 2】



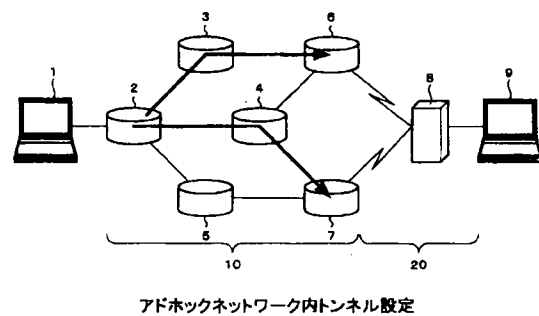
【図 3】



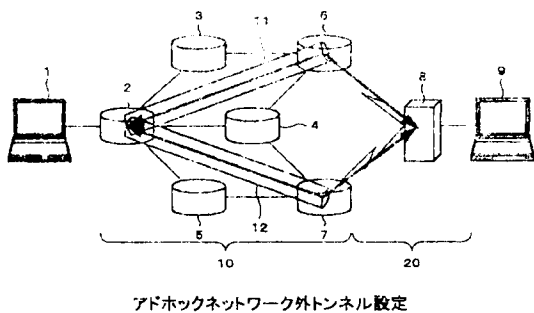
【図 4】



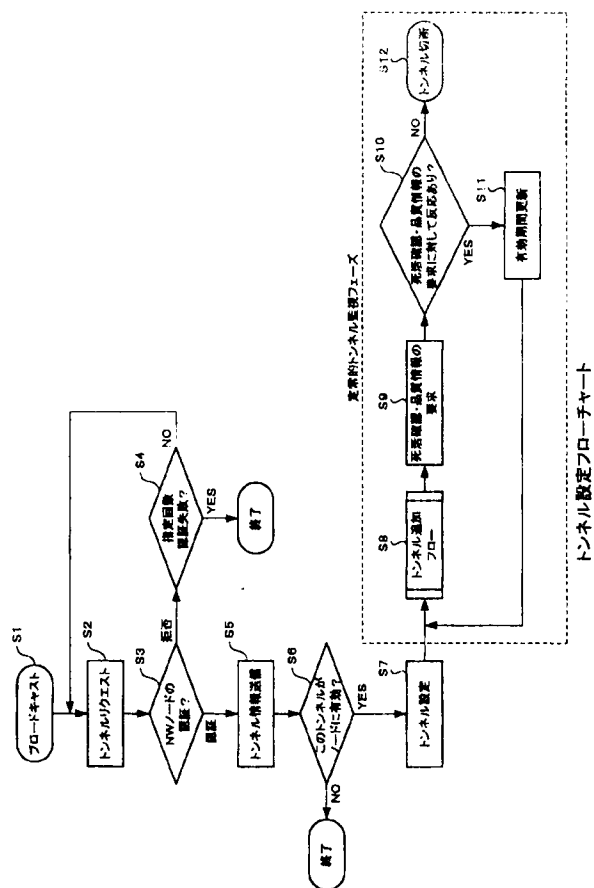
【図 5】



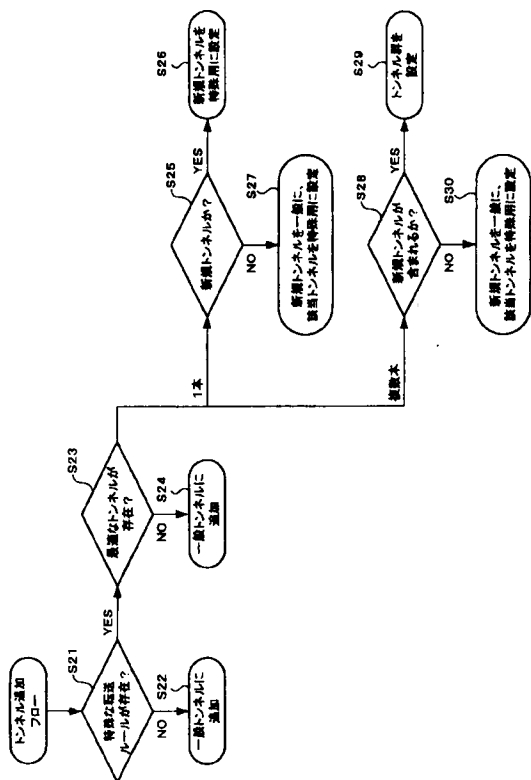
【図 6】



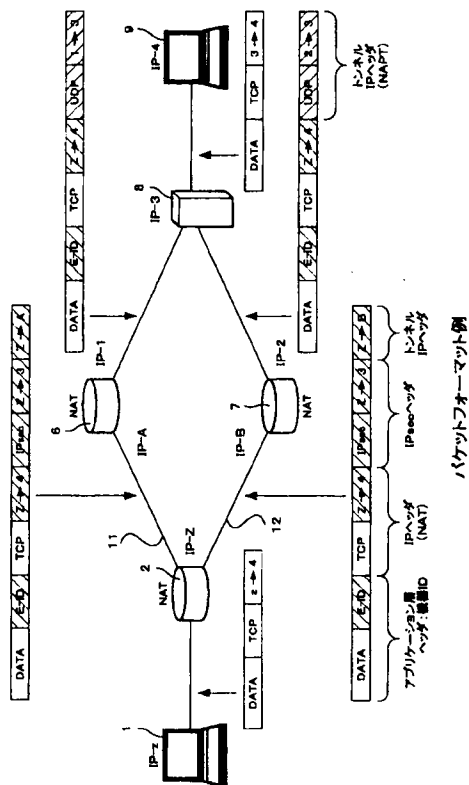
【図 7】



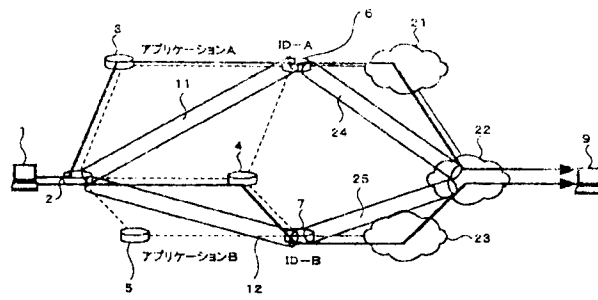
【図 8】



【図 9】



【図10】



通信経路選択の説明図

【図12】

ID	IP	遅延	損失	割当帯域	測定時刻
A	10.0.0.1	25ms	0.1%	100kbps	2003/07/01 12:15
B	10.0.1.1	40ms	1.2%	500kbps	2003/07/01 12:15
C	10.0.2.1	30ms	2.4%	250kbps	2003/07/01 12:15
D	10.0.3.1	10ms	1.5%	100kbps	2003/07/01 12:15
E	10.0.4.1	50ms	0.4%	200kbps	2003/07/01 12:15

トンネル情報データベース

【図11】

アプリケーション	DSCP	遅延	損失	帯域	セッション
VoIP	AF	100ms	0.5%	64kbps	3
ストリーミング	EF11	500ms	2%	200kbps	2
一般	BE	-	-	-	-

アプリケーションデータベース